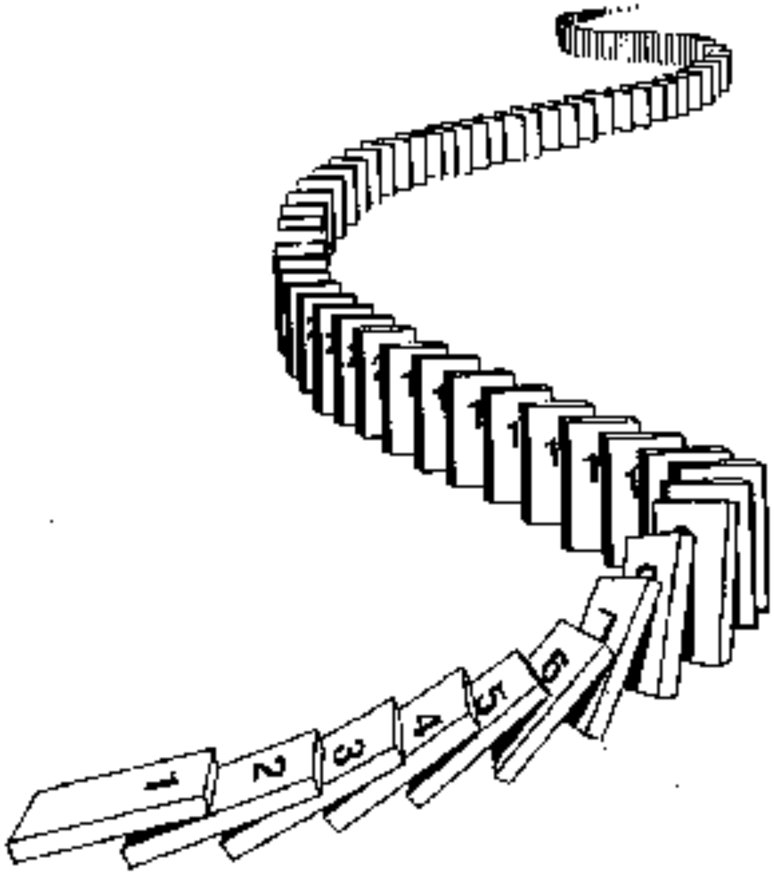
CSE 311: Foundations of Computing

Lecture 16: Fast modular exponentiation and Induction



Recap from last lecture

- **Bezout's Theorem.** For positive integers a and b, there are integers s and t so that $\gcd(a, b) = sa + tb$.
- **Extended Euclidean algorithm:** Finds a triple (g, s, t) so that $g = \gcd(a, b) = sa + tb$.

Recap from last lecture

- **Bezout's Theorem.** For positive integers a and b, there are integers s and t so that $\gcd(a, b) = sa + tb$.
- **Extended Euclidean algorithm:** Finds a triple (g, s, t) so that $g = \gcd(a, b) = sa + tb$.
- For integers a and $m \geq 1$, we call an integer b with $0 \leq b < m$ the **multiplicative inverse** if $ab \equiv 1 \pmod{m}$.
- If $1 = sa + tm$, then $s \,\%\, m$ is the multiplicative inverse of a modulo m.

Math mod a prime is especially nice

$\gcd(a,m) = 1$ if m is prime and $0 < a < m$ so can always solve these equations mod a prime.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

mod 7

Modular Exponentiation % 7

x	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

a	a^1	a^2	a^3	a^4	a^5	a^6
1						
2						
3						
4						
5						
6						

Modular Exponentiation % 7

x	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

a	a^1	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

Exponentiation

- **Compute** 78365^{81453}

- **Compute** 78365^{81453} % 104729

- **Output is small**
  - need to keep intermediate results small

Repeated Squaring – small and fast

Since $a \% m \equiv a \pmod{m}$ and $b \% m \equiv b \pmod{m}$

we have $ab \% m = \big((a \% m)(b \% m)\big)\% m$

So $a^2 \% m = (a \% m)^2 \% m$

and $a^4 \% m = (a^2 \% m)^2 \% m$

and $a^8 \% m = (a^4 \% m)^2 \% m$

and $a^{16} \% m = (a^8 \% m)^2 \% m$

and $a^{32} \% m = (a^{16} \% m)^2 \% m$

Can compute $a^k \% m$ for $k = 2^i$ in only i steps

What if k is not a power of 2?

Fast Exponentiation

```
public static long FastModExp(long a, long k, long modulus) {
       long result = 1;
       long temp;

       if (k > 0) {
           if ((k % 2) == 0) {
               temp = FastModExp(a,k/2,modulus);
               result = (temp * temp) % modulus;
           }
           else {
               temp = FastModExp(a,k-1,modulus);
               result = (a * temp) % modulus;
           }
       }
       return result;
   }
```

$$a^{2j} \% \, m = \left(a^j \, \% \, m\right)^2 \% \, m$$

$$a^{2j+1} \% \, m \; = \; \left((a \, \% \, m) \cdot (a^{2j} \, \% \, m)\right) \% \, m$$

The fast exponentiation algorithm computes $a^k \, \% \, m$ using $\leq 2 \log k$ multiplications $\% \, m$

Using Fast Modular Exponentiation

- Your e-commerce web transactions use SSL (Secure Socket Layer) based on RSA encryption
- RSA
  - Vendor chooses random 512-bit or 1024-bit primes p, q and 512/1024-bit exponent e. Computes $m = p \cdot q$
  - Vendor broadcasts (m, e)
  - To send a to vendor, you compute $C = a^e \ \% \ m$ using *fast modular exponentiation* and send C to the vendor.
  - Using secret p, q the vendor computes d that is the *multiplicative inverse* of e mod $(p-1)(q-1)$.
  - Vendor computes $C^d \ \% \ m$ using *fast modular exponentiation*.
  - **Fact:** $a = C^d \ \% \ m$ for $0 < a < m$ unless $p|a$ or $q|a$

Mathematical Induction

Method for proving statements about all natural numbers

- A new logical inference rule!
  - It only applies over the natural numbers
  - The idea is to **use** the special structure of the naturals to prove things more easily
- Particularly useful for reasoning about programs!

```
for(int i=0; i < n; n++) { … }
```

  - Show P(i) holds after i times through the loop

```
public int f(int x) {
    if (x == 0) { return 0; }
    else { return f(x – 1) + 1; }
}
```

  - f(x) = x for all values of $x \geq 0$ naturally shown by induction.

Prove $\forall a, b, m > 0\ \forall k \in \mathbb{N}\ (a \equiv b \pmod{m} \rightarrow a^k \equiv b^k \pmod{m})$

Let $a, b, m > 0 \in \mathbb{Z}$ be arbitrary. Let $k \in \mathbb{N}$ be arbitrary. Suppose that $a \equiv b \pmod{m}$.

We know $\big(a \equiv b \pmod{m} \wedge a \equiv b \pmod{m}\big) \rightarrow a^2 \equiv b^2 \pmod{m}$ by multiplying congruences. So, applying this repeatedly, we have:

$$\big(a \equiv b \pmod{m} \wedge a \equiv b \pmod{m}\big) \rightarrow a^2 \equiv b^2 \pmod{m}$$
$$\big(a^2 \equiv b^2 \pmod{m} \wedge a \equiv b \pmod{m}\big) \rightarrow a^3 \equiv b^3 \pmod{m}$$

…

$$\left(a^{k-1} \equiv b^{k-1} \pmod{m} \wedge a \equiv b \pmod{m}\right) \rightarrow a^k \equiv b^k \pmod{m}$$

The "…"s is a problem! We don't have a proof rule that allows us to say "do this over and over".

But there such a property of the natural numbers!

Domain: Natural Numbers

$$\frac{P(0) \qquad \forall k\,(P(k) \longrightarrow P(k+1))}{\therefore \forall n\; P(n)}$$

Induction Is A Rule of Inference

Domain: Natural Numbers

$$\frac{\begin{array}{c} P(0) \\ \forall k\ (P(k) \longrightarrow P(k+1)) \end{array}}{\therefore \forall n\ \ P(n)}$$

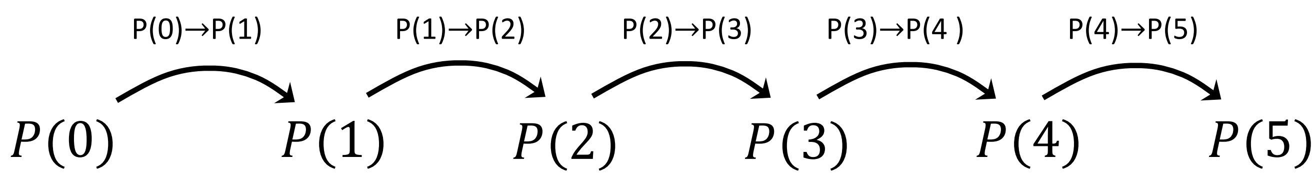
How do the givens prove P(5)?

Induction Is A Rule of Inference

Domain: Natural Numbers

$$\begin{array}{c} P(0) \\ \forall k\ (P(k) \longrightarrow P(k+1)) \\ \hline \therefore \forall n\ \ P(n) \end{array}$$

How do the givens prove P(5)?



First, we have P(0).

Since P(n) → P(n+1) for all n, we have P(0) → P(1).

Since P(0) is true and P(0) → P(1), by Modus Ponens, P(1) is true.

Since P(n) → P(n+1) for all n, we have P(1) → P(2).

Since P(1) is true and P(1) → P(2), by Modus Ponens, P(2) is true.

Using The Induction Rule In A Formal Proof

$$P(0)$$

$$\forall k\ (P(k) \longrightarrow P(k+1))$$

$$\therefore \forall n\ \ P(n)$$

Using The Induction Rule In A Formal Proof

$$\frac{P(0) \qquad \forall k\ (P(k) \longrightarrow P(k+1))}{\therefore \forall n\ \ P(n)}$$

1. Prove P(0)

4. $\forall$k (P(k) $\rightarrow$ P(k+1))
5. $\forall$n P(n) Induction: 1, 4

Using The Induction Rule In A Formal Proof

$$\frac{P(0) \qquad \forall k\ (P(k) \longrightarrow P(k+1))}{\therefore \forall n\ \ P(n)}$$

1. Prove P(0)
2. Let k be an arbitrary integer ≥ 0

3. $P(k) \rightarrow P(k+1)$
4. $\forall k\ (P(k) \rightarrow P(k+1))$ Intro $\forall$: 2, 3
5. $\forall n\ P(n)$ Induction: 1, 4

Using The Induction Rule In A Formal Proof

$$\frac{P(0) \qquad \forall k\ (P(k) \longrightarrow P(k+1))}{\therefore \forall n\ \ P(n)}$$

1. Prove P(0)
2. Let k be an arbitrary integer ≥ 0
    - 3.1. P(k) — Assumption
    - 3.2. ...
    - 3.3. P(k+1)
3. P(k) → P(k+1) — Direct Proof Rule
4. ∀k (P(k) → P(k+1)) — Intro ∀: 2, 3
5. ∀n P(n) — Induction: 1, 4

Translating to an English Proof

$$P(0)$$
$$\forall k\ (P(k) \longrightarrow P(k+1))$$
$$\therefore \forall n\ \ P(n)$$

1. Prove P(0) — **Base Case**

2. Let k be an arbitrary integer ≥ 0
    3.1. Suppose that P(k) is true

Inductive Hypothesis

    3.2. ...
    3.3. Prove P(k+1) is true

Inductive Step

3. $P(k) \rightarrow P(k+1)$ — Direct Proof Rule
4. $\forall k\ (P(k) \rightarrow P(k+1))$ — Intro ∀: 2, 3
5. $\forall n\ P(n)$ — Induction: 1, 4

Conclusion

Translating To An English Proof

1. Prove P(0) — **Base Case**

2. Let k be an arbitrary integer ≥ 0
    3.1. Assume that P(k) is true — **Inductive Hypothesis**

    3.2. ...
    3.3. Prove P(k+1) is true — **Inductive Step**

3.	$P(k) \rightarrow P(k+1)$	Direct Proof Rule
4.	$\forall k\,(P(k) \rightarrow P(k+1))$	Intro $\forall$: 2, 3
5.	$\forall n\, P(n)$	Induction: 1, 4

Conclusion

Induction Proof Template

[...Define P(n)...]

We will show that $P(n)$ is true for every $n \in \mathbb{N}$ by Induction.

Base Case: *[...proof of $P(0)$ here...]*

Induction Hypothesis:

Suppose that $P(k)$ is true for an arbitrary $k \in \mathbb{N}$.

Induction Step:

[...proof of $P(k+1)$ here...]

*The proof of $P(k+1)$ **can** invoke the IH somewhere.*

So, the claim is true by induction.

Inductive Proofs In 5 Easy Steps

Proof:

1. "Let $P(n)$ be... . We will show that $P(n)$ is true for every $n \geq 0$ by Induction."
2. "Base Case:" Prove $P(0)$
3. "Inductive Hypothesis:

   Suppose $P(k)$ is true for an arbitrary integer $k \geq 0$"
4. "Inductive Step:" Prove that $P(k+1)$ is true.

   Use the goal to figure out what you need.

   Make sure you are using I.H. and point out where you are using it. (Don't assume $P(k+1)$!!)
5. "Conclusion: Result follows by induction"

Prove $\sum_{i=0}^{n} i = n(n+1)/2$

1. **Let** P(n) **be "** $\sum_{i=0}^{n} i = n(n+1)/2$". **We will show** P(n) **is true for all natural numbers by induction.**

Prove $\sum_{i=0}^{n} i = n(n+1)/2$

1. **Let** P(n) **be** "$\sum_{i=0}^{n} i = n(n+1)/2$". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**

Prove $\sum_{i=0}^{n} i = n(n+1)/2$

1. **Let** P(n) **be "** $\sum_{i=0}^{n} i = n(n+1)/2$**". We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 0$**.**

Prove $\sum_{i=0}^{n} i = n(n+1)/2$

1. **Let** P(n) **be** "$\sum_{i=0}^{n} i = n(n+1)/2$". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** k ≥ 0**.**
4. **Induction Step:**

   Goal: Show $\sum_{i=0}^{k+1} i = (k+1)(k+2)/2$,

   which is exactly P(k+1)**.**

Prove $\sum_{i=0}^{n} i = n(n+1)/2$

1. **Let** P(n) **be** "$\sum_{i=0}^{n} i = n(n+1)/2$". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** k ≥ 0.
4. **Induction Step:**

$$\sum_{i=0}^{k+1} i = \sum_{i=0}^{k} i + (k+1)$$
$$= k(k+1)/2 + (k+1) \quad \textbf{by IH}$$
$$= (k+1)(k/2 + 1)$$
$$= (k+1)(k+2)/2$$

So, we have shown $\sum_{i=0}^{k+1} i = (k+1)(k+2)/2$,
which is exactly P(k+1).

Prove $\sum_{i=0}^{n} i = n(n+1)/2$

1. **Let** P(n) **be** “ $\sum_{i=0}^{n} i = n(n+1)/2$”. **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** k ≥ 0**.**
4. **Induction Step:**

$$\sum_{i=0}^{k+1} i = \sum_{i=0}^{k} i + (k+1)$$

$$= k(k+1)/2 + (k+1) \quad \textbf{by IH}$$

$$= (k+1)(k/2 + 1)$$

$$= (k+1)(k+2)/2$$

So, we have shown $\sum_{i=0}^{k+1} i = (k+1)(k+2)/2$,
which is exactly P(k+1)**.**

5. **Thus** P(n) **is true for all** n $\in \mathbb{N}$**, by induction.**

Lecture 16 Activity

- You will be assigned to **breakout rooms**. Please:
- Introduce yourself
- Choose someone to share screen, showing this PDF
- Complete the following proof:

1. Let P(n) be "$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$". We will show P(n) is true for all natural number by induction.
2. Base Case (n=0): .... so P(0) is true.
3. Induction Hypothesis: Suppose that P(k) is true for some arbitrary integer k ≥ 0.
4. Induction Step:

   We can calculate $\sum_{i=0}^{k+1} 2^i = \ldots\ldots.. = 2^{k+2} - 1$ using the Induction Hypothesis $P(k)$.
   This shows $P(k+1)$.
5. Thus P(n) is true for all n ∈ℕ, by induction.

Fill out a poll everywhere for Activity Credit!
Go to pollev.com/thomas311 and login
with your UW identity

Lecture 16 Activity

- You will be assigned to **breakout rooms**. Please:
- Introduce yourself
- Choose someone to share screen, showing this PDF
- Complete the following proof:

1. Let P(n) be ``$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$". We will show P(n) is true for all natural number by induction.
2. Base Case (n=0): $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$ so P(0) is true.
3. Induction Hypothesis: Suppose that P(k) is true for some arbitrary integer k ≥ 0.
4. Induction Step:

   We can calculate $\sum_{i=0}^{k+1} 2^i = \sum_{i=0}^{k} 2^i + 2^{k+1} = (2^{k+1} - 1) + 2^{k+1} = 2^{k+2} - 1$ using the Induction Hypothesis $P(k)$.

   This shows $P(k+1)$.
5. Thus P(n) is true for all n $\in \mathbb{N}$, by induction.

Fill out a poll everywhere for **Activity Credit**!
Go to pollev.com/thomas311 and login
with your UW identity

Another example of a pattern

- $2^0 - 1 = 1 - 1 = 0 = 3 \cdot 0$
- $2^2 - 1 = 4 - 1 = 3 = 3 \cdot 1$
- $2^4 - 1 = 16 - 1 = 15 = 3 \cdot 5$
- $2^6 - 1 = 64 - 1 = 63 = 3 \cdot 21$
- $2^8 - 1 = 256 - 1 = 255 = 3 \cdot 85$
- $\ldots$

Prove: $3 \mid (2^{2n} - 1)$ for all $n \geq 0$

Prove: $3 \mid (2^{2n}-1)$ for all $n \geq 0$

1. **Let** P(n) **be** “$3 \mid (2^{2n} - 1)$”. **We will show** P(n) **is true for all natural numbers by induction.**

Prove: $3 \mid (2^{2n} - 1)$ for all $n \geq 0$

1. **Let** P(n) **be** "$3 \mid (2^{2n} - 1)$". **We will show** P(n) i**s true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^{2 \cdot 0}-1=1-1=0=3 \cdot 0$ **Therefore** P(0) **is true**

Prove: $3 \mid (2^{2n} - 1)$ for all $n \geq 0$

1. **Let** P(n) **be** "$3 \mid (2^{2n} - 1)$". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^{2 \cdot 0} - 1 = 1 - 1 = 0 = 3 \cdot 0$ **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 0$.

I.e., suppose that $3 \mid (2^{2k} - 1)$

Prove: $3 \mid (2^{2n} - 1)$ for all $n \geq 0$

1. **Let** P(n) **be** "$3 \mid (2^{2n} - 1)$". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^{2\cdot 0}-1=1-1=0=3\cdot 0$ **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 0$.
4. **Induction Step:**

Goal: Show P(k+1), **i.e. show** $3 \mid (2^{2(k+1)} - 1)$

Prove: $3 \mid (2^{2n}-1)$ for all $n \geq 0$

1. **Let** P(n) **be** "$3 \mid (2^{2n} - 1)$". **We will show** P(n) i**s true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^{2\cdot 0}-1=1-1=0=3\cdot 0$ **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 0$**.**
4. **Induction Step:**

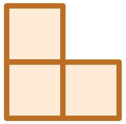
   By IH, $3 \mid (2^{2k} - 1)$ **so** $2^{2k} - 1 = 3j$ **for some integer** j

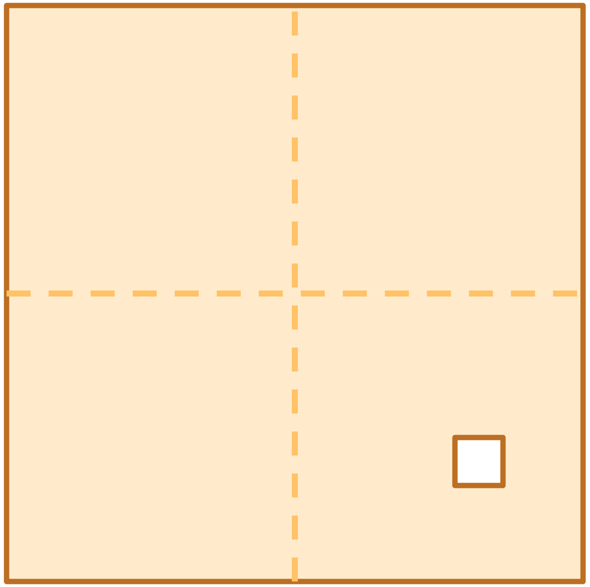
   So $2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 4(2^{2k}) - 1 = 4(3j+1) - 1$

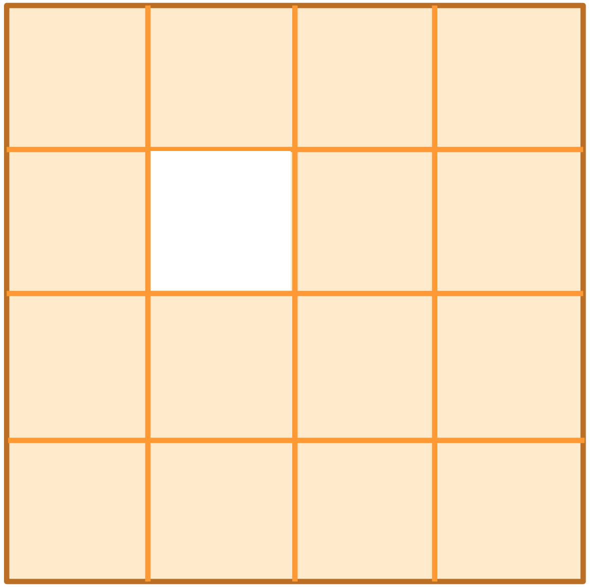
   $= 12j+3 = 3(4j+1)$

   Therefore $3 \mid (2^{2(k+1)} - 1)$ **which is exactly** P(k+1)**.**
5. **Thus** P(n) **is true for all** $n \in \mathbb{N}$**, by induction.**

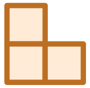
Checkerboard Tiling

- Prove that a $2^n \times 2^n$ checkerboard with one square removed can be tiled with: 

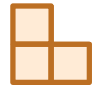
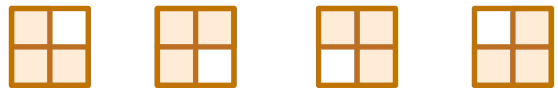


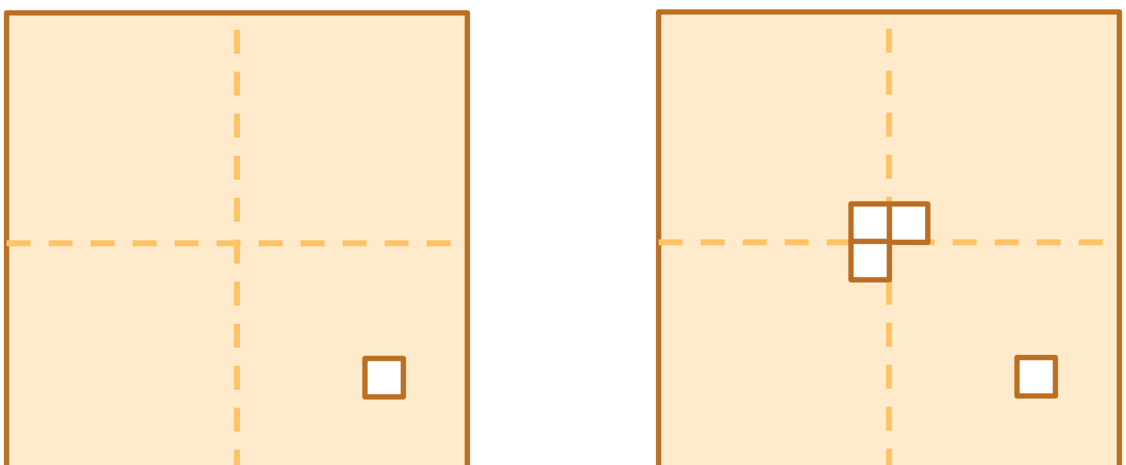


Checkerboard Tiling

1. Let $P(n)$ be any $2^n \times 2^n$ checkerboard with one square removed can be tiled with  .
   We prove $P(n)$ for all $n \geq 1$ by induction on n.
2. Base Case: $n=1$ 

Checkerboard Tiling

1. **Let** $P(n)$ **be any** $2^n \times 2^n$ **checkerboard with one square removed can be tiled with**  **.**
   We prove $P(n)$ **for all** $n \geq 1$ **by induction on** n.
2. **Base Case:** $n=1$ 
3. **Inductive Hypothesis: Assume** $P(k)$ **for some arbitrary integer** $k \geq 1$
4. **Inductive Step: Prove** $P(k+1)$



Apply IH to each quadrant then fill with extra tile.